ABSTRACT OF THE DISCLOSURE

The invention enables a registered PEAD user to exchange a secure message with another registered PEAD user by using the user ID and the user public key information in the server. The sender can retrieve the public key information from the server 1201 using the receiver's user ID as an index; then the sender can derive the shared secret using the receiver's public key. The sender then can encrypt the message with the shared secret and send it over to a server with the other PEAD user's (receiver's) ID appended with the sender's user ID over the wireless network and/or Internet. The server then stores the message and forwards the message to the receiver once the receiver's PEAD is polling for messages. (It is understood in the art that the server can push the messages to the receiver's PEAD).

The receiving PEAD user can use the sender's PEAD user ID and sender's public key information to derive the shared secret to decrypt a received secure message. Once a shared secret is computed or established by protocol between two users, that shared secret can be saved in the PEAD for future communication encryption/decryption usage.